Penetration Test Report: Calvin Blunk (*192.168.0.153*)
Author: Zach Maestas
Date of Assessment: 12.03.2025
Version: 1.0

Executive Summary

Overview

A penetration test was conducted against the student VM (192.168.0.153) to assess for vulnerabilities and weaknesses within their containerized services. The engagement identified a critical misconfiguration in the SSH service, allowing unauthorized root access. Additional services were enumerated but did not yield exploitable vulnerabilities.

High-Level Test Outcomes

The assessment successfully identified and exploited a critical weakness in the SSH service running on port 2222. Using the misconfiguration, full system compromise was achieved.

Overall Risk Rating

CRITICAL

Prioritized Recommendations

1. Disable SSH root login and enforce strong password authentication.
2. Implement key-based SSH authentication to prevent credential guessing.
3. Harden exposed services and remove unnecessary daemons (e.g., NoMachine, SMB).
4. Apply basic OS/Network hardening and review user/password configurations.

Test Scope and Methodology

Scope

The scope of this penetration test was the student's VM and its associated services. Additional exploitation was not attempted.

- **In-Scope Target:** 192.168.0.153
- **Out-of-Scope:** Any other devices on the network were explicitly out of scope. No denial-of-service (DoS) attacks were performed.

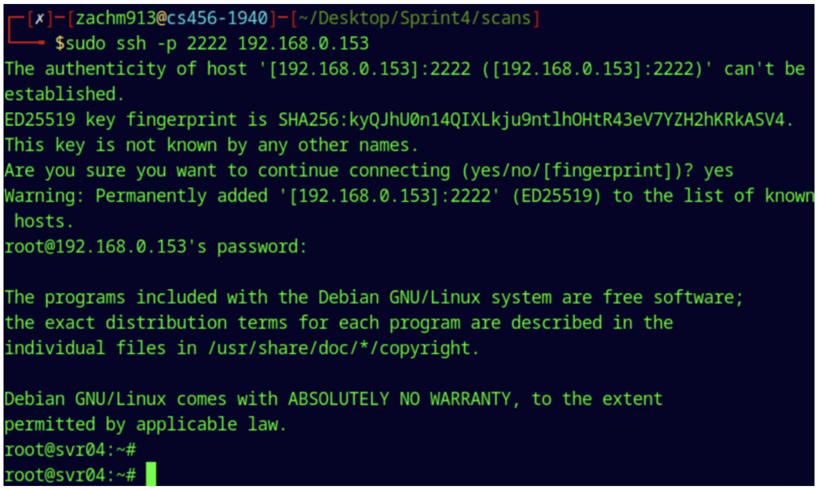
Methodology

Enumeration began with Nmap to identify open ports and running services. Each service was analyzed to determine whether it did in fact represent a likely vulnerability or decoy service. An analysis of SMB, NoMachine NX, and DVWA shows that those components were not viable avenues of exploitation. During this process, the SSH server listening on port 2222 was found allowing direct access to the root account via a blank login/password combination. This weakness was exploited and resulted in gaining access through the root account using a full root shell. All steps and evidence were recorded and included in the appendices.

Detailed Findings

3.1. Finding 1: Unauthorized Root Access via Weak SSH Configuration

- **Risk Rating:** Critical
- **Description:** The SSH port on 2222 permitted direct root authentication using a blank password. This misconfiguration allowed an attacker to gain immediate, full administrative access to the target VM with no brute force or privilege escalation required. This represents a total system compromise.
- **Affected Services/IPs:** SSH on TCP Port 2222 (192.168.0.153)
- **Evidence (Proof of Concept):**



```
┌─[✗]─[zachm913@cs456-1940]─[~/Desktop/Sprint4/scans]
└──╼ $sudo ssh -p 2222 192.168.0.153
The authenticity of host '[192.168.0.153]:2222 ([192.168.0.153]:2222)' can't be
established.
ED25519 key fingerprint is SHA256:kyQJhU0n14QIXLkju9ntlhOHtR43eV7YZH2hKRkASV4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.0.153]:2222' (ED25519) to the list of known
 hosts.
root@192.168.0.153's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@svr04:~#
root@svr04:~#
```

- **Remediation Steps:**
  - Disable root login in `/etc/ssh/sshd_config` (`PermitRootLogin no`)
  - Enforce strong passwords
  - Implement SSH key-based authentication
  - Restrict SSH to authorized IPs if possible
  - Rotate all passwords and audit user accounts

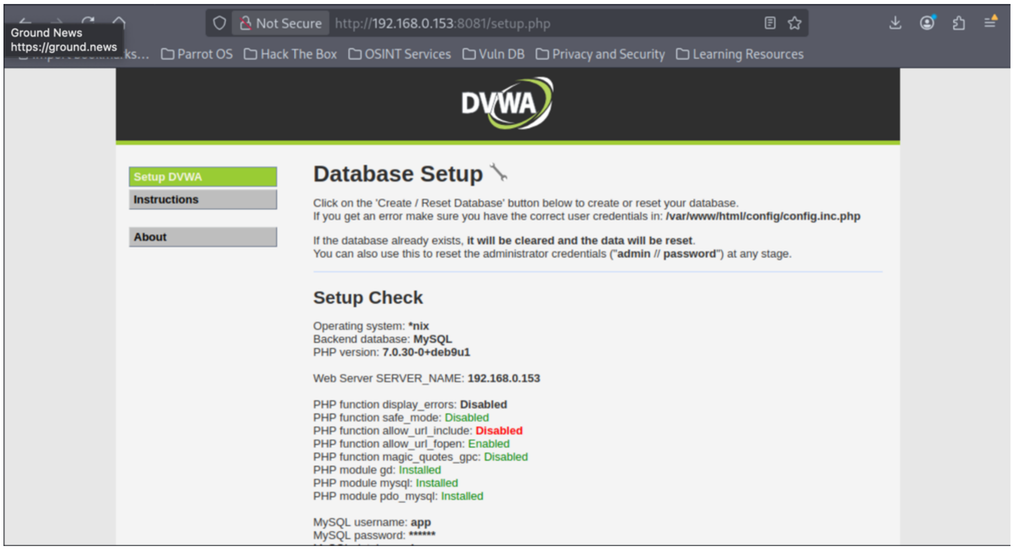
Failed Exploit Attempts

4.1. Attempt 1: SMB Enumeration

- **Service Targeted:** SMB on Port 445
- **Description of Attempt:** Ran SMB enumeration using smbclient -L.
- **Reason for Failure:** Service was properly configured and did not expose any exploitable vectors. Only default administrative shares (print$, IPC$) were available. No anonymous access or writable shares discovered.

4.2. Attempt 2: DVWA Setup Page

- **Service Targeted:** DVWA on Port 8081
- **Description of Attempt:** Identified DVWA but database was not initialized, preventing web exploitation paths. There was an open PHP login webpage, which is to be expected for DVWA.
- **Reason for Failure:** DVWA was not in a vulnerable operational state.
- **Screenshot:**



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/var/www/html/config/config.inc.php**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Operating system: ***nix**
Backend database: **MySQL**
PHP version: **7.0.30-0+deb9u1**

Web Server SERVER_NAME: **192.168.0.153**

PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: **app**
MySQL password: **********

Conclusions

Summary of Attack Path

The attacker used Nmap to enumerate services and identified SSH on port 2222 as a high-value target. Testing revealed the root account could authenticate with a blank or trivially weak password. This allowed immediate remote root shell access. From this point, full control over the system was achieved.

Overall Security Posture

The security posture of the VM is poor due to the presence of a critical SSH vulnerability that allows complete compromise with no resistance. Other services were configured more securely and did not present viable attack paths. Basic hardening and credential hygiene would have prevented the compromise.

Appendix

Tools Used

- Nmap
- smbclient
- SSH
- Browser (for DVWA)